Prepared, not delivered
Opening Statement

Chairman Michael G. Oxley
Committee on Financial Services

"Protecting our Financial Infrastructure: Preparation and Vigilance"
September 8, 2004

Saturday will mark the three-year anniversary of the terrible attacks of September 11. All of us remember that day and the dreadful uncertainties it brought.

Our nation's financial-services sector was able to withstand the stress and was quickly operational again. Much of the credit for that goes to the individuals who work in the industry, who spent countless hours to make sure that our nation's commercial lifeblood kept flowing with little or no interruption. Credit also goes to the business-protection and business-interruption planning and investment that began in the late 1990s as the nation prepared for the Y2K rollover.

While the quick recovery of U.S. market operations demonstrated the resilience of the American financial system, 9/11 exposed a laundry list of vulnerabilities. Though the loss of life and the physical destruction of the World Trade Center buildings were the most immediate consequence of the attacks, the threat to computer systems, telecommunications networks, electrical power grids, transportation systems, the paper check-clearing system and even water supplies supplying climate-control and computer-cooling systems was real.

We all know that those attacks may not be the last to rattle our country or our financial sector, and that potential business interruption may result from natural disasters — a hurricane, for example. Large catastrophic events like the train fire in Baltimore that severed a major East Coast telecommunications link, or the cascade of events that blacked out a large portion of the Northeast on August 14 of last year are also a serious consideration.

In the years since 9/11, the government and the private sector have worked unceasingly to strengthen the infrastructure that is critical to the functioning of our financial system. That infrastructure ranges from the physical, buildings that house banks and exchanges and clearing operations, to the computers that store and manipulate the data that is the lifeblood of our financial system, to the electrical power that runs those computers and the telecommunications lines along which that data runs.

Improved information-sharing, between industry and government and within the industry, has developed and refined "best practices" of protection and of business-resumption techniques.

Of course, efforts to protect the financial sector's critical infrastructure, like efforts to protect the country itself, can never cease. What was good enough as a protection against threats yesterday, must necessarily change tomorrow as the nature and type of threat changes. Intentional or accidental computer viruses and denial-of-service attacks by definition will be different tomorrow than today. Terrorists are determined and creative, and the risk of accident is always present.

Domestic efforts to strengthen our critical infrastructure are the first best defense. But America's leading role in the global financial system requires us also to keep an eye on how vulnerabilities abroad can affect our markets. Threats to our financial institutions and international financial organizations can emanate from anywhere and be transmitted through the Web. We need to be able to distinguish between terrorist threats and more fraud-oriented hacker threats. Both are serious, but they require different response mechanisms. Within the private sector, ensuring that counterparty relationships and back-up liquidity facilities exist in the event of extraordinary threats to the marketplace are critical components of a security plan as well as good business practice.

From that perspective, the limited, industry-specific and location-specific raising of the terror threat level, issued August 1 by Homeland Secretary Ridge, offers us an excellent illustration of the evolution of this process of protecting our critical financial infrastructure and the international organizations that are located in our country. Instead of raising the threat level for the entire nation, affected institutions and locations were alerted nearly instantly, as our witnesses will tell us today. The result was increased watchfulness where it was necessary, without undue anxiety or the unnecessary use of resources where it was not.

As the world becomes increasingly complex, and as financial markets become increasingly global and inter-related, I am glad we have dedicated public servants, and smart, hard-working folks in the private sector focused on this issue. We have several of them here today as witnesses to tell us how far we have come in the protection of our critical financial infrastructure, what we must yet do, and how Congress can help.